LISTING OF CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment, comprising the steps of:

(a) creating a public-private key pair within the secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message;

(b) storing the private key within the device against the possibility of divulgement thereof by the device; and

(c) securely linking the public key with other information by storing the public key in association with the other information in a database within the secure environment.

2. (Original) The method of claim 1, wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device.

3. (Original) The method of claim 2, wherein each digital signature generated by each device is a random number.

4. (Currently amended) The method of claim 1 ~~2~~, wherein the other information comprises respective security features and a manufacturing history of each device.

5. (Currently amended) The method of claim 1 ~~2~~, further comprising the step of identifying a particular manufactured device by authenticating a message using one of a plurality of public keys in the database within the secure environment ~~one of said linked public keys~~, a digital signature for the message having been generated by the particular manufactured device.

6. (Withdrawn)(Cancelled) ~~A method of maintaining a Central Key Authority (CKA) database, the CKA database comprising PuK-linked account information of users, the PuK-linked account information maintained in the database for each user including:~~

~~(a) a public key of a user device that generates digital signatures,~~

~~(b) information securely linked with the public key of the device during manufacturing of the device in a secure environment, and~~

~~(c) third-party account identifiers each of which identifies to a third-party an account of the user that is maintained with the third-party and that has been associated with the user's public key by the third-party.~~

7. (Withdrawn)(Cancelled) ~~The method of claim 6, wherein the information linked with the public key comprises security features and a manufacturing history of the device.~~

8. (Withdrawn)(Cancelled) ~~The method of claim 6, wherein the public key and information linked therewith is obtained from a Secure Entity.~~

9. (Withdrawn)(Cancelled) ~~The method of claim 6, wherein the PuK-linked account information maintained in the CKA database for each user further includes the identity of each third-party with which an account is maintained that is identified by one of the third-party account identifiers.~~

10. (Withdrawn)(Cancelled) ~~The method of claim 6, wherein the PuK-linked account information of the users is indexed in the CKA database by unique CKA account~~

~~identifiers such that the PuK-linked account information for a user is retrievable from the CKA database based on the account identifier.~~

11. (Withdrawn)(Cancelled) ~~The method of claim 10, wherein the public key is the unique account identifier.~~

12. (Withdrawn)(Cancelled) ~~The method of claim 6, wherein the PuK-lined account information maintained in the CKA database for each user further includes user-specific information, and further CKA database for each user further includes user-specific information, and further comprising the step of verifying the user-specific information.~~

13. (Withdrawn)(Cancelled) ~~The method of claim 12, wherein each user account further includes a record of the techniques that were employed in verifying the user-specific information.~~

14. (Withdrawn)(Cancelled) ~~The method of claim 12, wherein the user-specific information includes the name and address of the user.~~

15. (Withdrawn)(Cancelled) ~~The method of claim 12, wherein the user-specific information includes the age and gender of the user.~~

16. (Withdrawn)(Cancelled) ~~The method of claim 6, further comprising establishing an account on behalf of a user with a third-party by communicating the public key of the user and information linked with the public key from the CKA database to the third-party.~~

17. (Withdrawn)(Cancelled) ~~The method of claim 16, wherein the public key of the user and information linked with the public key is communicated upon the request of the third-party to which it is communicated.~~

18. (Withdrawn)(Cancelled) ~~The method of claim 6, further comprising updating PuK-linked accounts of a user maintained with at least two independent third-parties with a new public key of the user, comprising the steps of:~~

~~(a) receiving an EC, the EC including one of the CKA account identifiers and a message including the new public key and a digital signature therefor;~~

~~(b) authenticating the message of the EC using the public key associated with the account in the CKA database identified by the CKA account identifier, and upon successful authentication thereof;~~

~~(c) sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the CKA database and associated with the account identified by the CKA account identifier.~~

19. (Withdrawn)(Cancelled) ~~The method of claim 18, further comprising digitally signing the new public key of the user and third-party account identifier.~~

20. (Withdrawn)(Cancelled) ~~The method of claim 18, further comprising sending the EC received from the user to each of the third-parties.~~

21. (New) The method of claim 1, wherein the public key and information linked therewith is obtained from a Secure Entity.

22. (New) The method of claim 1, wherein the PuK-linked information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

23. (New) The method of claim 22, wherein the PuK-linked account information of the users is indexed in the database by unique account identifiers such that the PuK-linked account information for a user is retrievable from the database based on the account identifier.

24. (New) The method of claim 22, wherein the public key is the unique account identifier.

25. (New) The method of claim 1, wherein the PuK-linked information maintained in the database for each user further includes user-specific information..

26. (New) The method of claim 12, wherein the user-specific information includes the name and address of the user.

27. (New) The method of claim 6, further comprising the step of establishing an account on behalf of a user of a device with a third-party by communicating the public key of the device and the other information linked with the public key from the database to the third-party.

28. (New) The method of claim 27, wherein the public key of the device and the other information linked with the public key is communicated to a third party upon the request of the third-party.

29. (New) The method of claim 1, further comprising the step of updating the PuK-linked accounts of a user maintained with at least two independent third-parties with a new public key of the user, comprising the steps of:

(a) receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefor,

(b) authenticating the message of the EC using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof,

(c) sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier.

30. (New) The method of claim 29, further comprising the step of digitally signing a message involving the new public key of the user and a third-party account identifier.

31. (New) The method of claim 29, further comprising the step of sending the EC received from the user to each of the third-parties.